America's Health Insurance Plans

601 Pennsylvania Avenue, NW
South Building
Suite Five Hundred
Washington, DC 20004

202.778.3200
www.ahip.org

January 19, 2007

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: Identity Theft Task Force
Solicitation of Public Comments

Dear Sir or Madam:

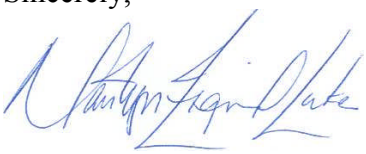
America's Health Insurance Plans (AHIP) is writing to offer comments in response to the Identity Theft Task Force Request for Comments that was posted on the U.S. Department of Justice website at http://www.usdoj.gov/ittf/.

AHIP is the national association representing nearly 1,300 health insurance plans providing coverage to more than 200 million Americans. Our members offer a broad range of products in the commercial marketplace including health, long-term care, dental, vision, disability, and supplemental coverage. Our members also have a strong track record of participation in Medicare, Medicaid, and other public programs. Virtually all of our members are covered entities for purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and comply with HIPAA's privacy and security regulatory requirements and other federal and state laws which set comprehensive requirements for health insurance plans to ensure the privacy and security of individually identifiable information.

AHIP supports the work of the Identity Theft Task Force to coordinate the development of a strategic plan for improving the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. We have reviewed the Request for Comments and offer our comments and recommendations in the attached document (Attachment A).

We appreciate the opportunity to comment on these important issues. Please contact me by phone at (202) 861-1473 or by email at mzigmundluke@ahip.org with any questions.

Sincerely,



Marilyn Zigmund Luke
Associate Regulatory Counsel

Attachment A

Identity Theft Task Force
Solicitation of Public Comments
Response of America's Health Insurance Plans

AHIP offers the following comments and recommendations in response to the Request for Comments that was issued by the Identity Theft Task Force. The sections and issues highlighted below correspond with those noted in the solicitation.

Maintaining Security of Consumer Data

Issue 1: Federal agencies should follow the lead of the private sector and restrict the public display of confidential individual information, such as Social Security numbers (SSNs).

Discussion 1: When the Identity Theft Task Force issued interim recommendations in the fall of 2006, one of the main recommendations was that federal agencies should examine the use and collection of SSNs since those numbers are often used in committing identity theft. The Request for Comments indicates that the Task Force is currently considering whether additional measures should be taken by both the public and private sectors to further enhance the protection of SSNs and other sensitive consumer information.

Health insurance plans are accustomed to and conscientious about protecting confidential individual data and health information. Existing federal laws including the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and corresponding regulatory requirements require health insurance plans to have policies and procedures in place to protect the privacy and security of individually identifiable health information. State laws and regulations often mirror the federal requirements or require private health insurance plans to implement privacy and security protections for individually identifiable information that are more stringent than the federal requirements.

As an example, historically health plans and insurers used SSNs as an individual identifier on insurance cards, certain member communications, and in electronic business transactions. However, as a result of the legal and regulatory requirements and as an innovative business practice to protect consumers' information, health insurance plans began to "phase out" the public display of SSNs. As a matter of general business practice, non-descript public identifiers have routinely replaced the traditional public disclosure of SSNs. In some instances, however, federal and state agencies have not implemented similar protections for SSNs and other types of individually identifiable information.

Recommendation 1: The federal Identity Theft Task Force recommendations for reducing the occurrence of identity theft should suggest that both the public and private sectors follow similar legal requirements that limit the public disclosure of SSNs and other types of individually identifiable information. The Task Force should recommend that Congress and the federal executive agencies use existing legal requirements and business practices to implement such protections.

Issue 2: National individual identifiers (other than SSNs) should be developed for use by business industry segments, as appropriate.

Discussion 2: As discussed above, some health care and other industries have historically used SSNs to identify individuals in business transactions. While SSNs were not intended to be used routinely by public or private entities, the availability and public disclosures of these identifiers in business transactions made them attractive tools for thieves to use in identity crimes.

A more practical alternative to using SSNs may be to allow each industry (health care, financial services, etc.) the ability to develop and use individual identifiers specific to the industry segment. Using national identifiers helps ensure that individuals are appropriately "matched" to their corporate records when services are provided and business transactions occur. In addition, national identifiers help entities authenticate that an individual is who he or she claims to be.

If different identifiers were developed by various industry segments, this could prevent multiple uses of a SSN or other individually identifiable information used to commit identity theft and other crimes. For example, the HIPAA statute mandated that a national patient identifier be developed for use in identifying individuals in health care settings and transactions. The HIPAA patient identifier may be an effective deterrent for some types of identity theft because the identifier cannot be re-used to commit multiple fraudulent transactions (such as to fraudulently obtain medical care and then fraudulently obtain credit or a loan).

Recommendation 2: A national, strategic plan to prevent identity theft should include recommendations for using individual identifiers by business industry segment. For the health care industry, a national patient identifier as required by HIPAA should continue to be explored.

Issue 3: A federal strategic plan for preventing identity theft should include uniform, clearly-defined standards for private and public entities that do not duplicate existing statutory and regulatory requirements and business practices which ensure the privacy and security of individually identifiable data. These standards should include an appropriate mechanism for federal oversight and enforcement.

Discussion 3: The Request for Comments indicates that the Task Force is considering recommending that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. In addition, the Task Force is

considering whether to recommend that a national breach notification requirement be adopted.

Health insurance plans already comply with HIPAA requirements for preventing, detecting, and responding to data security incidents. The HIPAA security requirements require entities to develop and maintain security policies and procedures, train members of their workforce, and have processes in place to detect and receive reports about suspected security incidents. When security incidents occur, entities can evaluate the individual facts and circumstances of each incident. The HIPAA security standards enable entities to investigate whether a breach of data has, in fact, occurred and to develop an appropriate response to mitigate any harmful results to individuals or the entity. The HIPAA Security Rule is an effective basis for private entities in addressing data security requirements.

While AHIP supports HIPAA as a national, federal standard for ensuring the privacy and security of individually identifiable data, the current regulatory environment can be complex. Private health insurance plans are currently subject to multiple federal and state statutory and regulatory requirements governing privacy and security requirements that protect individually identifiable data. Often these requirements govern the privacy of specific types of information (e.g., health information related to HIV status), mandate technical or business processes to ensure the security of information (e.g., state laws governing data breach notifications), and establish federal and state mechanisms for jurisdiction, oversight and enforcement. Because of these consistencies, our members have always taken the position that a federal data security standard is preferable.

While a federal data security standard is a preferred approach, we encourage the Task Force to recommend that a strategic plan evaluate the most effective and efficient ways that enforcement of a national data security standard can be accomplished for all industries. Defining what constitutes a "data breach" can vary depending upon the business industry and the legal requirements governing the entity or the information. One approach may be to allow oversight and enforcement by existing regulatory agencies. For example, the U.S. Department of Health and Human Services is an appropriate oversight agency for data security issues for health care entities. However, it is not clear how federal enforcement could be effectively accomplished if more than one federal agency has enforcement jurisdiction.

In addition, any federal data standard for providing individual notification in the event of a data breach should be crafted so that the specific facts and circumstances surrounding a data breach can be taken into consideration by a private entity that is attempting to appropriately respond. Factors that could be considered may include: whether a reasonable likelihood of identity theft or other unlawful conduct exists following the breach; the number of individuals affected by a data breach; the type of information that was the subject of the breach; the size and financial resources of the private entity; whether the data was protected through encryption or other technical means; and whether a criminal investigation is pending. These as well as other factors can help private

entities, law enforcement, and regulators evaluate the most effective and timely responses to protect individuals from identity theft or other harm.

Recommendation 3: The Task Force should recommend that a strategic plan to prevent identity theft include uniform, clearly-defined standards based on existing statutory and regulatory requirements and business practices for private and public entities in ensuring the privacy and security of individually identifiable data. This recommendation should include convening a public forum for business industry leaders to evaluate the most-effective and efficient mechanisms for: (1) enforcing a national data security standard across public and private industries; and (2) providing guidelines for notifying individuals in the event of a data breach.

Issue 4: Public and private entities, as well as individuals can benefit from information about ways to prevent, detect, and respond to identity theft.

Discussion 4: The Task Force has solicited input about whether there is a need to educate the private sector about safeguarding information and what private sector entities should do if a data breach occurs. Additionally, the Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft through a national public awareness campaign.

Ongoing, national educational efforts identifying current trends in crimes involving identity theft will help private entities develop better systems, policies, and practices to detect, report, and deter identity theft. Such educational efforts can help entities develop innovative ways to thwart identity thieves and protect individuals.

Consumers are also empowered by educational efforts addressing identity theft schemes. Such information can help individual consumers protect themselves through early detection and reporting when identity theft occurs. Such educational efforts empower individual consumers and enable them to work with public and private entities and law enforcement in the ongoing battle against identity theft.

Recommendation 4: We urge the federal government to consider educational efforts, such as a national public awareness campaign for the private sector and individuals about safeguarding information to detect and deter identity theft.

Victim Recovery

Issue 5: An adequate framework exists for individuals to pursue criminal enforcement mechanisms if an identity crime is committed against them.

Discussion 5: The Request for Comments solicits input about whether existing statutes should be modified or new statutes created to enable individuals the ability to seek restitution or recovery in the event that their identity is compromised.

Current federal and state laws and regulations provide individuals with appropriate mechanisms to have suspected instances of identity theft criminally investigated and prosecuted. Pursuing an individual who has committed identity theft through civil legal remedies will likely be a futile and frustrating exercise for individuals to undertake.

As the Request for Comments recognizes, in many situations an identity thief will be outside the jurisdiction of U.S. courts because he or she is located in a foreign country and cannot be effectively served with notice of a lawsuit filed in a U.S. court. In other situations, even if an individual consumer hires legal counsel and wins a civil judgment, the identity thief is likely to be "judgment proof" – meaning that there is no likelihood that the individual consumer will be able to collect on his or her civil judgment. And as long as private entities have taken reasonable steps to protect individually identifiable information, it is unreasonable to hold private entities liable for the criminal actions of individuals.

Recommendation 5: The Identity Theft Task Force should recommend that a national strategic plan addressing identity theft include information for individuals, law enforcement, and prosecutors about ways to initiate criminal investigations and enforcement mechanisms when identity theft occurs.

Law Enforcement

Issue 6: Public and private entities as well as individuals can benefit from statistical information about identity theft.

Discussion 6: AHIP supports the work of the Identity Theft Task Force to examine ways to implement the requirements of the Executive Order by addressing identity theft through "increased aggressive law enforcement actions," but there are limited data available that effectively summarize statistics about the law enforcement investigations or prosecutions relating to identity theft.

Recommendation 6: The Task Force should recommend that a federal study be conducted to gather data on: (1) the types of crimes that are occurring involving identity theft, including information about the industries, individuals, and geographic areas being affected; (2) whether and how often these crimes are successfully investigated and prosecuted; and (3) whether law enforcement and prosecutors can identify specific reasons that may prevent investigating or pursuing an identity theft case. The results of such a study should be publicly disseminated.